Administering Avaya Aura™ Communication Manager as a Feature Server

03-603479
Issue 1.3
Release 5.2
March 2010

© 2010 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

Concurrent User License

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya Aura™ System Manager, and Avaya Aura™ Session Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: Overview....7
Communication Manager as a Feature Server....7
Communication Manager as a Trunk Gateway....7
Supported features....8

Chapter 2: Configuring Communication Manager as a Feature Server....11
Adding a node name....11
Adding an IP network region....11
Adding a SIP signaling group....12
Changing dial plan TAC....12
Adding a SIP trunk group....13
Numbering....13
Administering numbering....13

Chapter 3: Administering the Feature Server on System Manager....17

Chapter 4: Adding users....21

Chapter 5: Feature Name Extension Administration....23
Administering Feature Name Extensions on the SAT....23
Administering Feature Name Extensions on System Manager....23

Chapter 6: SIP Phone administration....25
Administering 96xx SIP phones....25

Index....27

Chapter 1: Overview

This document explains how to configure and administer Avaya Aura™ Communication Manager as a Feature Server, how to add users, and how to administer the 96xx SIP phones.

On Communication Manager, there can be two types of signaling connections to Avaya Aura™ Session Manager:

- IMS (IP Multimedia Services)
- Non-IMS

Calls from one signaling group cannot route over the other. Non-IMS calls must remain non-IMS, and IMS calls must remain IMS. Cross-mixing of functionalities is not supported.

Communication Manager as a Feature Server

Communication Manager as a Feature Server only supports IMS-SIP users that are registered to Avaya Aura™ Session Manager. The Communication Manager server is connected to Session Manager via an IMS-enabled SIP signaling group and associated SIP trunk group.

Communication Manager as a Feature Server has the following constraints:

- The dial plan for IMS users must route all PSTN calls back to Session Manager over the IMS trunk group. Routing of such calls directly to ISDN trunks is not supported.
- SIP trunks and SIP endpoints are supported
- The supported SIP phone sets are the 96xx and 96xx SIP phones. The preferred type is 96xxSIP.
- ESS and LSP are not supported
- IPSI port networks are not supported
- Traditional phones such as DCP, H.323, ISDN, and analog are not supported.

Communication Manager as a Trunk Gateway

Communication Manager can function simultaneously as a Trunk Gateway and a Feature Server. This requires that the **IMS Enabled** field on the signaling group screen be set to **n.**

Careful provisioning of the dial plans and locations must be made to keep the two roles separate.

Supported features

The following features are supported for Communication Manager as a Feature Server:

Feature	Description
Voicemail	One mailbox per user supporting MWI for lamp-on, lamp-off, and interrogation.
Basic Calling	Normal call setup and teardown.
Hold (including Music on Hold)	Users may place calls on hold. The hold treatment (music, silence, tones) are provided by Communication Manager.
Multiple Line Appearances	Users may handle at least 4 calls delivered to the same line and can move from call to call using the hold and un-hold functions.
Call Transfer	Users may transfer calls either by pressing the **transfer** button or using an **on-hook**.
Ad-hoc Conference	Up to 6 party conferences are supported. Both consultative (private connection between the conferencing party and the party to be conferenced in) and blind conferences (conferences before the conferenced party answers) are supported.
Drop	Drop last party on conference. Selective drop is not supported.
Call Restrictions	The current restrictions for incoming calls, outgoing calls, outgoing toll calls, and calls to selected communities of endpoints are supported.
Return Call	Each user is responsible for maintaining the call log and the user interface to display and select a particular call.
Distinctive Alerting	User can be alerted for incoming calls as inside the enterprise network, outside the enterprise network, and priority calls.
Call Forwarding (unconditional, busy/no answer)	Call forwarding works as it does today.
Hunt Groups	Hunt groups whose members are entirely controlled by the same Communication Manager are supported. All existing types of hunt groups are supported.

Feature	Description
Simultaneous Ring	Communication Manager users can be associated with multiple phones (for example, OPTIM EC500 cellular phone) and all will ring simultaneously.
Outgoing Caller ID	Outgoing Caller ID is supported.
Emergency Service Routing	Emergency Service Routing is supported.
Incoming Caller ID	Incoming Caller ID is supported.
Hold Recall	The user receives a re-alert on a line appearance if it has been held longer than the administered time.
Call Pickup	All users are able to pickup calls using call pickup. Directed call pickup, group call pickup, and extended call pickup are supported. The pickup group may not span multiple Communication Managers.
Meet-me Conference	All users can join meet-me conferencing bridges. Up to 6 parties per meet-me conference are supported.
Do not disturb — send all calls (SAC)	Send all calls feature activations are supported for both primary extensions and bridged appearances.
Whisper Page	All users except those with third party phones can make and receive whisper pages. Users can whisper page and accept whisper pages from phones belonging to the same Communication Manager.
Transfer Recall	A call transferred to another user will return to the transferring user after the administered period of time. The recall will re-alert the station that the transfer did not complete.
Bridged Appearances	Phones visibly indicate the status of calls on call appearances native to other stations. Users may **`bridge-on`** to calls on these **`bridged appearances`**. This feature only applies to groups of stations served by the same Communication Manager.
One Touch Recording	The One Touch Recording feature works on bridged appearances, not just primary appearances. The storage for the One Touch Recording is Modular Messaging.
Priority Calling	Users can originate a call as a priority call.
Call Coverage	Calls to a user that are not answered or the user is busy follow a set pattern of coverage. Calls can be redirected to any number both on and off the enterprise.
Auto Redial	Incoming and outgoing calls in the user's call log can be redialed from the user's interface.
Busy Indicator (attendant line monitoring)	The user can have an indicator of another user's on/off hook status.

Feature	Description
Call Park and Unpark	Users can park and unpark a call. The two users that park and unpark a call must be controlled by the same Communication Manager.
Abbreviated Dial	Any user may use dial codes to access personal, group, and server-wide abbreviated dial groups.
Authorization Codes	Any user may enter an authorization code for each call originated. The authorization codes are administered by the system administrator.
Account codes	Users may use an account code for each call originated. The account codes are administered by the system administrator.

Chapter 2: Configuring Communication Manager as a Feature Server

There are two places where you administer Communication Manager. One is as an RTS application, the other as a Session Manager application for application sequencing.

This section describes how to administer Communication Manager using the SAT to define the connection and routing between Session Manager and Communication Manager as a Feature Server. The following sections need to be administered in the order given.

Adding a node name

Define a node name for the IP address of the Session Manager SM100 board.

1. Enter `change node-names ip`
2. Enter a node name (Name) for the IP Address of the Session Manager SM100 board.
3. Enter the IP address of the Session Manager SM100 board.
4. Submit the screen.

Adding an IP network region

Define an IP network region that will be referred to in the signaling group to Session Manager (defined later).

1. Enter `change ip-network-region` *n*
2. Enter the domain name in the **Authoritative Domain** field (e.g., fr.rnd.avaya.com)

3. Enter the name in the **Name** field.
4. Submit the screen.

Adding a SIP signaling group

Set up a SIP signaling group with IMS enabled from the feature server Communication Manager procr to the Session Manager SM100 board.

1. Enter `add signaling-group` *`next`*
2. Enter `sip` for the **Group Type**.
3. Set **IMS Enabled?** to `y`.
4. Set **Near-end Node Name** to `procr`.
5. Set **Far-end Node Name** to the Session Manager *SM100–hostname*.
6. Set **Far-end Domain** to the domain name entered as the **Authoritative Domain** in the step above.
7. Set **Enable Layer 3 Test?** to `y`.

   If this field is set to `n`, the links will not be monitored by Communication Manager.
8. Submit the screen.

Changing dial plan TAC

Before you can add a trunk group, you must select a trunk access code (TAC) value for the group to be created.

1. Enter **change dialplan analysis**
2. Enter a TAC dial string to be used for the trunks.
3. Submit the screen.

Adding a SIP trunk group

Add a SIP trunk group to the SIP signaling group defined for the connection from the Communication Manager Feature Server to Session Manager.

1. Enter `add trunk-group` *`next`*
2. On the trunk group screen, enter `sip` for the **Group Type**.
3. For **Signaling Group**, enter the signaling group number that was previously assigned.
4. Add as many trunk members as needed.
5. Submit the screen.

Numbering

Feature server users need to be added in either the private or public numbering table. The rules to adapt and evaluate numbering in the IMS environment are as follows:

1. Look in the public numbering table. If a match is found, extend the number and add a plus ("+"). The extension must be in the international format. e.g. 1303 or 49211 etc.
2. If no match is found in the public numbering table, look in the private numbering table. If a match is found, extend the number. Any extension is possible, as long as it makes the number enterprise canonical.

Administering numbering

Enter the internal numbers without the prefix to the private or public numbering table. Create an entry for all used trunk groups, or create only one entry with a blank trunk group field.

If the call number is public, create an entry in the public numbering table.

1. Enter `change system-parameters customer-options`
2. Set **Private Networking** to `y` if it is not already enabled.

3. Go to Page 2.
4. Set a value for **Max Administered SIP Trunks.**
5. Enter **newterm** to make the changes take effect.
6. Log back into the SAT.
7. Enter `change private-numbering x`
8. Enter the number which corresponds to the extension length allowed by the dial plan in the **Ext Len** field.
9. Enter the leading extension digits in the **Extension Code** field.

   The entry cannot be longer than the number entered in the **Ext Len** field.
10. Enter a valid administered trunk group or a range of trunk groups in the **Trk Grp(s)** field or leave this field blank. A blank field means the entered information applies to all trunk groups.
11. If you are using the enterprise canonical numbering scheme in Session Manager, enter the prefix to the Communication Manager extension in the **Private Prefix** field . If Session Manager and Communication Manager are using the short Communication Manager extension, leave this field blank.
12. Enter the **Total Len**
13. Submit the screen.
14. For each station:
    a. Enter `change station x`
    b. The **Phone Type** should be 96xxSIP
    c. Go to Page 6 of the station form.
    d. Under **SIP Trunk option**, specify either the trunk number (administered above) or **aar.**
    e. Submit the screen.
    f. If using aar, the appropriate screens need to be changed.

       In AAR analysis, define an entry for each call number or a pattern of call numbers that point to a route-pattern which routes to the trunk group, administered above. This trunk group, which is associated with the signaling group that points to the relevant Session Manager, is the **first and only** entry in the route pattern.
    g. If using short Communication Manager extension and enterprise canonical in the core, enter `change inc-call-handling-trmt trunk-group x` and modify the appropriate information for **Incoming Len**, **Number of Digits**, and **Del**
    h. Make sure that **public-unknown-numbering** does not overlap with **private-numbering**

i. Enter `change off—pbx—telephone station-mapping x`
j. If you use the enterprise canonical numbering scheme in Session Manager, enter the extension's enterprise canonical number in the **phone number** field. The phone number is the number the user registers with.
k. Submit the screen.
l. If using enterprise canonical on both Communication Manager and Session Manager, no more steps are required. Otherwise, continue with the **Numbering** section.

Chapter 3: Administering the Feature Server on System Manager

1. Install a Session Manager if it does not already exist. For the installation procedures, see *Installing and Upgrading Avaya Aura™ Session Manager,* 03–603473.
2. Log on to the System Manager console if you have not logged on already.
3. Administer the Session Manager as a SIP entity:
    a. Select **Network Routing Policy** > **SIP Entities**
    b. Select **New**
    c. Enter the Name of the Session Manager in the **Name** field
    d. Enter the IP Address of the SM100 board of the Session Manager in the **FQDN or IP Address** field.
    e. Select **Session Manager** from the drop-down menu in the **Type** field.
    f. Under the **Port** section, click **Add**
    g. Add port 5060, protocol TCP
    h. Click **Add**
    i. Add port 5061, protocol TLS
    j. Select the two ports and click **Commit**
4. Administer the Session Manager if it has not already been administered:
    a. Select **Session Manager** > **Session Manager Administration**
    b. Select **Add**
    c. Enter the SIP entity name (Name of the Session Manager), IP address (IP address of the Session Manager), and other required information. You must administer the SIP entity through the NRP pages. The SIP entity address is the IP address of the SM-100 board.
    d. Make sure the **Enable Monitoring** box is checked. This allows the links to be monitored.
    e. Click **Commit**
5. Add the Feature Server SIP domains in the Network Routing Policy:
    a. Select **Network Routing Policy** > **SIP Domains**

   b. Click **New**
   c. Enter the domain name for the Communication Manager.
   d. Select `cm` from the drop-down menu in the **Type** field.
   e. Click **Commit**
   f. Click **New**
   g. Enter the domain name for the Session Manager.
   h. Select `sip` from the drop-down menu in the **Type** field.
   i. Click **Commit**

6. Administer the Communication Manager as a SIP entity:
   a. Select **Network Routing Policy** > **SIP Entities**
   b. Select **New**
   c. Enter the Name of the Communication Manager
   d. Enter the IP Address of the Communication Manager. The IP address is the near-end in the signaling group to Session Manager.
   e. Select **CM** from the drop-down menu in the **Type** field.
   f. Click **Commit**
7. Create an entity link from the Session Manager entity to the Communication Manager entity:
   a. Select **Network Routing Policy** > **Entity Links**
   b. Select **New**
   c. Enter a name to be associated with the Entity Link.
   d. For **SIP Entity 1**, select the Session Manager entity from the drop-down menu.
   e. For **SIP Entity 2**, select the entity for the Communication Manager feature server that was just created from the drop-down menu.
   f. Select **Commit**
8. Administer Communication Manager as an application:
   a. Select **Applications** > **Entities**
   b. Select **New**
   c. Select **CM** from the drop-down menu in the **Type** field.
   d. In the **Application** section, enter the Name of the Communication Manager.
   e. Select **Other** from the drop-down menu in the **Node** field.
   f. Enter the IP address of the Communication Manager in the **Other Node** field (the IP address that is used for the SAT login).

    g. In the **Attributes** section, enter a login and password of a user account created on your Communication Manager for the purpose of PPM (and other) communication between Communication Manager and Session Manager.

    Note:

    If this user account has not already been created in Communication Manager, it needs to be created for proper SIP endpoint communication. The user account type is “18”, or super user type.

    h. Make sure the **Is SSH Connection** box is checked.
    i. Make sure the port is **5022**
    j. Under **Attributes**, enter a login and a password for Communication Manager (SAT SSH login and password).
    k. Select **Commit** — this causes synchronization to run in the background.
    l. Select **Communication System Management** > **Telephony**. The Communication Manager Element should be displayed in the table.

9. Create an application for the application sequence:
    a. Select **Session Manager** > **Application Configuration** > **Applications**
    b. Select **New**
    c. Enter the application **Name**.
    d. Select the **SIP Entity** for Communication Manager. The other fields are optional.
    e. Select **Commit**
10. Create an Application Sequence:
    a. Select **Session Manager** > **Application Configuration** > **Application Sequences**
    b. Select **New**
    c. Under **Available Applications**, click the + sign in front of the appropriate instance.
    d. When the screen refreshes, make sure the **Mandatory** box is checked.
    e. Select **Commit**
11. Check if the links are up:
    a. Select **System Status** > **SIP Entity Monitoring**
    b. Check if the links are up (Entity Links Down/Total).
12. Synchronize the data to System Manager:
    a. Select **Communication System Management** > **Telephony**
    b. Select the appropriate Element name.

c. Select **Initialize data for selected devices**

d. Select **Now**.

   It may take several hours to complete the synchronization. Synchronization will occur incrementally after this and will not take as long to complete.

Chapter 4: Adding users

The following are the steps for adding users. Any input fields not mentioned in the steps can be ignored. There are a number of input fields which are not necessary for Session Manager user administration.

A user may have more than one Communication Profile. For more information regarding the fields, see the on-line help.

---

1. Select **User Management** > **User Management**
2. Select **New**.
3. In the **General** section, enter the user's last name and first name.
4. Enter a description in the **Description** field. This field is optional.
5. Select a **User Type**
6. In the **Identity** section, enter a **Login** name.

   This is the unique system login name given to the user. It takes the form of username@domain (enterprise canonical number) and is used to create the user's primary handle.
7. The **Authentication Type** should be `Basic`
8. Enter an **SMGR Login Password** and confirm it. The password must start with an alpha (lower or upper case) character.
9. The **Shared Communication Profile Password** *must* be administered. The password must be all numeric characters. This is the password that is used when logging in to the phone.
10. Enter the **Localized Display Name** of the user. This is the name that is displayed as the calling party.
11. Enter the full text name of the user for **Endpoint Display Name**
12. Click on the show/hide button for **Communication Profile**
13. Click on the show/hide button for **Communication Address**
14. For each SIP handle:
    a. Select **New**.
    b. Select `sip` from the drop-down menu for **Type** if it is not set already.
    c. In the **SubType** field, select `username` from the drop-down menu. If the handle is a full E.164 number, select the `e164` subtype. msrtc is currently not used.

    d. In the **Fully Qualified Address** field, enter the extension number.
    e. Select **Add**.
15. Assign the user to a Communication Manager station:

    Note:
    This step cannot be done until synchronization of the data has completed.

    a. Click the show/hide button next to **Station Profile**
    b. Check the box to the left of **Station Profile**
    c. Select the Communication Manager from the **System** drop-down menu.
    d. Check **Use Existing Stations** if the station already exists on the Communication Manager that is associated with this user.

       The box must be checked in order to associate the user with the selected Communication Manager station settings. Otherwise, leave the box unchecked to create a station automatically .
    e. Enter the extension that is administered on Communication Manager for the existing or new station in the **Extension** field.
    f. Enter a port in the **Port** field.
    g. Select the **Delete Station on Unassign of Station from User** box.
16. Under the Session Manager section:
    a. Make sure the **Session Manager** check box is checked.
    b. Select the appropriate Session Manager instance from the drop-down menu in the **Session Manager Instance** field.
    c. Select the appropriate application name from the drop-down menu in the **Origination Application Sequence** field.
    d. Select the appropriate application name from the drop-down menu in the **Termination Application Sequence** field.
17. Select **Commit**.

Next steps

Administer the SIP phone associated with the user.

Chapter 5: Feature Name Extension Administration

The following steps describe how to administer feature name extensions. Feature name extensions must first be administered on the Communication Manager SAT, then administered for Session Manager using the System Manager web interface.

Administering Feature Name Extensions on the SAT

On the SAT:

1. Enter `change feature-access-codes`
2. Enter the appropriate codes for the features you want to enable.
3. Submit the screen.
4. Enter `change off-pbx-telephone feature-name-extensions set` *1*
5. Enter the number you want to use for a particular feature (xxx-xxxx).
6. Submit the screen.

Administering Feature Name Extensions on System Manager

On the System Manager console:

1. Select **Session Manager** > **Application Configuration** > **Implicit Users**
2. Select **New**
3. Enter a phone number in the **Pattern** field (xxx-xxxx)
4. Enter the Minimum number of digits to be matched by the system in the **Min** field.

5. Enter the Maximum number of digits to be matched by the system in the **Max** field.
6. Enter a description in the **Description** field. For example, Turn on EC500.
7. Select the appropriate **SIP Domain** from the drop-down menu.
8. Select the appropriate originating feature server name from the **Origination Application Sequence** drop-down menu.
9. Select the appropriate terminating feature server name from the **Termination Application Sequence** drop-down menu.
10. Click **Commit**

Chapter 6: SIP Phone administration

This section contains the administration procedures for the 96xx SIP phones used for Communication Manager as a Feature Server.

Administering 96xx SIP phones

The 96xx SIP phones should have the GA version of firmware 2.5 installed.

The phone can also download settings from a file server if the environment is set up.

1. Go to the configuration menu:
    a. On the hard phone: Press the **Mute** button on the phone and use the keypad to enter **CRAFT#**
    b. On the soft phone: Enter `admin options`
2. In **SIP Global Settings** of the phone configuration menu, set the **SIP Domain** to the domain of your Session Manager environment.
3. Set the **Avaya Environment** to `auto`.
4. Leave the **Avaya Config Server** setting blank.
5. In **SIP Proxy Settings**, add an entry for the Session Manager the phone should register to with the IP address of the Session Manager SM100 board.
6. In **SIP Proxy Settings**, set **Transport** to `TCP, TLS,` or `UDP`.
7. In **SIP Proxy Settings**, set the port as defined in the Session Manager SIP Entity (usually 5060).
8. To access the correct file server:
    a. Navigate to **Admin Procedures**
    b. Select **SSON**
    c. Enter the SSON.

Index

Numerics

96xx SIP phone administration 25

A

add trunk-group 13
adding users 21

C

Communication Manager, Feature Server constraints ... 7

F

feature access codes 23
feature name extension administration 23
Feature Name Extension administration 23
Feature Server administration, System Manager 17
feature-name-extensions 23
FNE administration on System Manager 23

I

IP Network Region 11
ip-network-region 11

L

legal notice 2

N

node-name, adding 11
numbering administration 13
numbering rules 13
numbering, ...13

S

SIP phone administration 25
SIP phone administration, 96xx 25
System Manager administration for CM Feature Server 17

T

TAC 12
trunk access code 12
Trunk Gateway overview 7

U

users, adding 21